Jennifer A. Hradil, Esq.
Justin T. Quinn, Esq.
GIBBONS P.C.
One Gateway Center
Newark, NJ 07102-5310
(973) 596-4500

Eugene F. Assaf, P.C., DC Bar 449778
Pro Hac Vice
K. Winn Allen, DC Bar 1000590
Pro Hac Vice
KIRKLAND & ELLIS, LLP
655 Fifteenth St. N.W.
Washington, D.C. 20005
(202) 879-5078
eugene.assaf@kirkland.com
winn.allen@kirkland.com

Douglas H. Meal, MA Bar 340971
Pro Hac Vice
ROPES & GRAY, LLP
Prudential Tower, 800 Boylston Street
Boston, MA 02199-3600
(617) 951-7517
douglas.meal@ropesgray.com
Attorneys for Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

FEDERAL TRADE COMMISSION Plaintiff, v. WYNDHAM WORLDWIDE CORPORATION, et al., Defendants.	Civil Action No.: 2:13-cv-01887-ES-SCM **REPLY IN SUPPORT OF MOTION TO DISMISS BY DEFENDANT WYNDHAM HOTELS & RESORTS LLC** **ORAL ARGUMENT REQUESTED** **MOTION DATE JUNE 17, 2013**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

Statutes

Treatises

INTRODUCTION

The FTC has appointed itself as a roving data-security prosecutor—but, unlike other prosecutors, the FTC itself defines the elements of the offense and does so only after the fact. Worse, the FTC turns victims of cybercrime into defendants by bringing "case-by-case," quasi-criminal enforcement proceedings against companies like Wyndham, which responded to cyberattacks in a responsible fashion by alerting law enforcement, notifying consumers, retaining experts, and spending millions on remedial measures. The FTC, however, is not letting the law or the facts get in the way of its data-security agenda. The lesson for American businesses (large and small) is clear: do not expect the FTC to say what the rules are until after your business has been attacked, had data stolen, participated in an investigation, and been subjected to litigation.

That theory of governmental power is fundamentally inconsistent with the principles of fair notice and due process that are at the core of our legal system. If the rule of law means anything, it means the government must say in advance what the rules are before it tries to impose liability for breaking them. "We know it when we see it" is not a lawful (or desirable) approach to agency regulation. *See* Stegmaier, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements*, 20 GEO. MASON L. REV. 673 (2013). It is no answer to say, as the FTC does, that "reasonableness is the touchstone" of a Section 5 violation. Opp. 17. In the highly complex and technically sophisticated world of data security, a command to "act reasonably" provides no guidance as to how businesses must manage their systems, program their software, configure their servers, or make any of the other decisions involved in protecting computer networks from hackers.

The FTC dismisses WHR's objections as the complaints of a company that purportedly failed to "lock the doors of the store at night." *Id.* at 9. The FTC knows better. Hacking is an endemic, unavoidable problem in the modern world, as the scores of recent cyberattacks against private companies and government agencies show. Public Citizen Br. at 4 (621 confirmed data breaches in 2012 alone); GAO, *Information Security* (2011), *available at* http://www.gao.gov/assets/590

/585570.pdf. Subsequent to the attacks that victimized WHR, the FTC itself was attacked by cybercriminals, as was the FBI, CIA, and DOD. Surely the FTC does not seriously argue that these agencies—not to mention Google, CitiBank, Sony, and scores of other sophisticated companies—are leaving their doors open to cybercriminals. The way to help victims of cybercrime is not to empower the FTC to scour the country for "unreasonable" data-security practices, particularly when (as here) there is no evidence that consumers suffered economic harm from the attacks. It is, as Congress and the President have recognized, to establish in advance clear data-security requirements by which companies should abide and to allow companies to share information without the chill of litigation. Those ongoing efforts by the Executive and Legislative branches only confirm that Section 5, to the extent it even applies in the data-security context, provides no meaningful guidance as to what a business can do to comply with the law.

I. THE COUNT II UNFAIRNESS CLAIM MUST BE DISMISSED

A. The FTC's Unfairness Authority Does Not Extend To Data Security

The FTC, like any other federal agency, bears the burden of showing that Congress intended to delegate to it the specific authority it claims. *See Louisiana Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986). The FTC, however, points to no explicit grant of authority to regulate data security under Section 5. Instead, it argues that "Congress deliberately delegated broad power to the FTC under Section 5" and points to ***other*** contexts in which the FTC has "use[d] … its unfairness provision." Opp. 11. Those arguments fail for three reasons. *See American Bar Ass'n v. FTC*, 430 F.3d 457, 468 (D.C. Cir. 2005) (FTC lacks authority to regulate attorneys under the GLB Act).

First, the notion that Section 5 authorizes the FTC to act as a roving prosecutor of data security is "inconsistent with the intent that Congress has expressed … in the [data-security] specific legislation that it has enacted subsequent" to the FTC Act, which allocate specific data-security responsibilities to specific federal agencies in specific economic sectors. *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 126 (2000). Those statutes do much more than simply

provide the FTC with "new legal tools," such as "rulemaking and/or civil penalty authority."[1] Opp. 12. The FCRA, GLB Act, and COPPA contain detailed provisions explicitly authorizing the FTC to set substantive standards regarding data security, *see* 15 U.S.C. §§ 1681m(e)(1), 6804(a)(1)(C), 6502(b), and to enforce those standards under Section 5 of the FTC Act, *see* 15 U.S.C. §§ 1681s(a), 6805(a)(7), 6505(d). Those provisions would have been entirely unnecessary if, as the FTC claims, Congress believed Section 5 already afforded the FTC such authority. Congress's limited delegation of data-security authority to other federal agencies likewise would make little sense if the FTC already enjoyed the broad data-security powers it claims. *See* MTD at 9-10.

Second, the FTC cannot run away from its previous admissions that it lacks jurisdiction over data security. The FTC offers no response at all to an FTC official's 2001 statement that "'[t]he agency's jurisdiction is (over) deception…. If a practice isn't deceptive, we can't prohibit them from collecting information.'" Benner, *FTC Powerless to Protect Privacy*, Wired. And although the Privacy Report observes that the "FTC Act prohibits unfair and deceptive practices," the very same paragraph explains that, in the data-security context, the FTC is limited to its deception jurisdiction and "lacks authority to require firms to adopt information practice policies." 2000 FTC Privacy Report at 37. Nor can the FTC dismiss Chairman Pitofsky's disavowal of regulatory authority as being limited to "online privacy." Opp. 14. Chairman Pitofsky's remarks applied to the "privacy ***and security*** of … personal information," and called for legislation requiring entities "to take reasonable steps to protect the ***security*** and integrity of [personal] information." *Consumer Privacy on the World Wide Web*, 105th Cong. (July 21, 1998) (emphases added). No such legislation would have been necessary if the Commission already had such authority under Section 5.

Third, the ongoing political debate about data-security regulation belies the notion that Congress intended the FTC to use Section 5 to set data-security standards. Although it

[1] The FTC ***already has*** rulemaking authority under Section 5 of the FTC Act. *See* 15 USC § 57a(A).

acknowledges that debate, the FTC argues that Congress has ***acquiesced*** in FTC regulation through "inaction." Opp. 13, 17. The Supreme Court, however, has often "expressed skepticism toward reading the tea leaves of Congressional inaction," because what the FTC describes as "Congress's deliberate acquiescence should more appropriately be called Congress's failure to express any opinion." *Rapanos v. United States*, 547 U.S. 715, 749-50 (2006). The Court has thus demanded "***overwhelming*** evidence" that Congress "considered and rejected the ***precise*** issue presented before the Court" before it will rely on congressional silence. *Id*. at 750 (emphases added). There is no evidence—much less "overwhelming evidence"—that Congress specifically considered and approved the FTC's use of Section 5 to impose data-security standards on the private sector.[2]

Although the FTC suggests otherwise, Opp. 16-17, this Court owes no deference to the FTC's newfound interpretation of Section 5 because the FTC has not engaged in formal adjudication or rulemaking. *United States v. Mead Corp.*, 533 U.S. 218, 227 (2001); *FCC v. Arlington*, 2013 WL 2149789, at *10 (S. Ct. 2013) ("*Mead* denied *Chevron* deference to action, by an agency with rulemaking authority, that was not rulemaking"). And even if deference were appropriate, courts nevertheless should not hesitate to overturn "an agency's expansive construction of the extent of its own power [which] would … [work] a fundamental change in the regulatory scheme." *Id*. at *9.

B. The FTC Refuses To Give Fair Notice Of What The Law Requires

Section 5 also does not permit the FTC to bring data-security enforcement actions without first publishing rules or regulations explaining in advance what parties must do to comply with the law. Stegmaier, 20 GEO. MASON L. REV. 673. "A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or

[2] The FTC relies on four proposed bills and a single statement from a sponsor of one of those bills. Opp. 15-16. None of those bills addressed, much less endorsed, the FTC's claimed authority under Section 5. And the "savings clauses" in those bills more sensibly refer to the FTC's narrow delegations under the FCRA, GLBA, and COPPA. Congress has also considered ***six other*** cybersecurity bills that included no language at all "preserving" data-security authority for the FTC. *See* S. 1151, S. 1408, S. 1434, S. 1535; S. 2105; H.R. 624.

required." *FCC v. Fox Telev. Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012). The FTC's approach—which amounts to "we know a data-security violation when we see it"—is the opposite of fair notice.

The Commission nonetheless asks the Court to overlook the absence of fair notice because, by the Commission's telling, it is too difficult to specify in advance what data-security practices a company must adopt. *See* Opp. 20. But that only proves WHR's point. Providing fair notice to private citizens and businesses should matter ***more***, not less, when the regulating agency itself struggles to separate lawful from unlawful conduct. It is thus unsurprising that the Commission points to ***no*** case holding that the government can abandon its fair-notice obligations merely because it finds it challenging to articulate governing legal standards.

In truth, however, the FTC overstates the difficulty it would encounter in providing advance notice. The Commission has in the past issued data-security rules after notice-and-comment rulemaking in a number of discrete areas. For example:

- 16 C.F.R. Pt. 314 sets forth specific standards under the GLB Act "for developing, implementing, and maintaining reasonable" technical safeguards to protect consumer information. 16 C.F.R. § 314.1; *see also id*. § 314.4.
- 16 C.F.R. Pt. 682 implements the FCRA by articulating specific guidelines regarding the proper destruction of consumer information. *See* 16 C.F.R. § 682.3.

There is no reason the FTC could not announce similar *ex ante* rules here—other than the FTC's admission that it prefers the "regulatory flexibility" of employing a vague standard such as "reasonableness." Opp. 21. But unchecked discretion is not a virtue of the FTC's current approach to Section 5. It is the very reason that such a regime cannot be lawful.

When an agency tries to make new law through enforcement actions (as the FTC is doing here), it generally cannot simultaneously hold a party liable for violating the newly announced rule. *See Gates & Fox Co. v. OSHRC*, 790 F.2d 154, 156 (D.C. Cir. 1986). Under Third Circuit law, it can do so ***only*** when the agency has previously stated with "ascertainable certainty" the standards it expects private parties to obey. *Dravo Corp. v. OSHRC*, 613 F.2d 1227, 1233 (3d Cir. 1980).

The FTC's proffered legal standard falls woefully short of the "ascertainable certainty" threshold. In the Commission's words, "reasonableness is the touchstone" of a data-security violation under Section 5: "unreasonable data security practices are unfair." Opp. 17. But in the highly complex and sophisticated world of data security, a mere "reasonableness" standard provides no guidance at all. Applying such a standard, there is no way WHR could know what software configurations it must employ, Am. Compl. ¶ 24(b), how it must set up firewalls, *id*. ¶ 24(a), what password complexity standards it must adopt, *id.* ¶ 24(f), how it must inventory computers connected to the network, ¶ 24(g), how it must program servers, *id*. ¶ 24(d), or how it must make any of the other decisions that go into implementing a data-security program.

Conceding that "reasonableness" alone is not sufficient, the FTC argues that WHR could have consulted the FTC's prior consent decrees.[3] Those consent orders, however, contain little more than highly abstract statements about the defendants' data-security practices. *See, e.g.*, *In the Matter of The TJX Companies, Inc.*, No. 072 3055, ¶ 8 (faulting TJX for not using "readily available" techniques to limit wireless access or "sufficient measures" to prevent unauthorized access); *In the Matter of Guidance Software, Inc.*, No. 062 3057, ¶ 8 (faulting Guidance for not "adequately assess[ing]" the vulnerability of its network, using "readily available security measures," or employing "sufficient measures" to detect unauthorized access); *In the Matter of DSW Inc.*, No. 052 3096 ¶ 7 (similar). And, according to the complaints in those cases, it is only when each of the alleged data-security deficiencies are "taken together" that they become "unfair." *See id*. The public is thus left to wonder which combination of vaguely identified deficiencies results in liability.

[3] Private standards cannot provide the fair notice the FTC has refused to give. Voluntary industry standards are not law and do not purport to reveal what the FTC (or any other entity) believes Section 5 to require. *See, e.g.*, *Romero v. Buhimschi*, 2007 WL 2902896 (E.D. Mich. 2007) ("Plaintiff has failed to demonstrate that the voluntary adoption of private standards of conduct creates a legal duty."); Standards.org, *PCI DSS* ("PCI DSS is not law.").

In any event, the Commission's consent orders cannot substitute for an agency statement carrying the force of law. As the FTC concedes, Opp. 19, its prior consent orders are not "controlling precedent for later Commission action" that in any way limit the FTC's enforcement powers. *Beatrice Foods Co. v. FTC*, 540 F.2d 303, 312 (7th Cir. 1976); *Intergraph Corp. v. Intel Corp.*, 253 F.3d 695, 698 (Fed. Cir. 2001) ("[A] consent order does not establish illegal conduct."). Statements that do not constrain governmental authority do not provide the fair notice that due process requires. *See City of Chicago v. Morales*, 527 U.S. 41, 63-64 (1999).

The FTC attempts to excuse its failure to provide fair notice by drawing analogies between Section 5's "unfairness" language and the good-faith-bargaining provision of the NLRA and the "General Duty Clause" in OSHA. Opp. 23. Unlike data-security regulation under Section 5, the duty to negotiate in good faith has a long-established meaning in contract law. *Katsiavrias v. Cendant Corp.*, 2009 WL 872172, at *6 (D.N.J. 2009); UCC § 1-201(20) (defining "good faith"). Similarly, there are over 30 years of concrete, specific agency guidelines specifying the obligations imposed by the General Duty Clause. *See Con Agra, Inc.*, 1983-84 O.S.H. Dec. (CCH) ¶ 26,420, at 33, 523 (1983). And even despite that guidance, courts have dismissed on fair-notice grounds numerous agency enforcement actions applying occupational-safety regulations that are far more specific than the General Duty Clause. *See, e.g.*, *Fabi Constr. Co. v. Secretary of Labor*, 508 F.3d 1077, 1088 (D.C. Cir. 2007); *Gates & Fox*, 790 F.2d at 156; *Dravo*, 613 F.2d at 1232-33.[4]

The FTC incorrectly asserts that it has no fair-notice obligation in this case because it is not seeking civil penalties. But due process concerns do not evaporate merely because the agency is seeking disgorgement and highly burdensome injunctive relief in lieu of civil penalties. *See UAW v. Bagwell*, 512 U.S. 821, 836-38 (1994). To the contrary, courts frequently dismiss agency actions on

[4] *General Elec. Co. v. Gilbert*, 429 U.S. 125 (1976), is not a fair-notice case and, in any event, consent orders did not make the Supreme Court's list of "informed judgment[s] to which courts and litigants may properly resort for guidance." *Id.* at 141-42.

fair notice grounds even when the agency is not seeking civil penalties or other punitive remedies. *See United States v. Chrysler Corp.* 158 F.3d 1350, 1355-56 (D.C. Cir. 1998) (car recall); *In re Bogese*, 303 F.3d 1362, 1368 (Fed. Cir. 2002) (forfeiture); *PMD Produce Brokerage v. USDA*, 234 F.3d 48, 51 (D.C. Cir. 2000) (license revocation); *Trinity Broad. v. FCC*, 211 F.3d 618, 619 (D.C. Cir. 2000) (license renewal); *Satellite Broad. Co. v. FCC*, 824 F.2d 1, 3 (D.C. Cir. 1987) (same).

Under the FTC's view, filing a data-security enforcement action is no burdensome task. All the Commission need do is allege that a defendant acted "unreasonably" and make conclusory claims that the defendant failed to adopt "proper" or "adequate" technologies. Because no rules or regulations exist cabining the FTC's authority, no defendant could ever establish at the pleading stage that the FTC's lawsuit contravened controlling law. FTC data-security actions, in other words, would be exempted from Rule 12(b)(6) scrutiny.

When WHR's network was attacked in 2008, it had no fair notice of what network architecture, firewalls, inventory procedures, and incident-response plans the FTC believed Section 5 required. Even today the FTC still cannot (or will not) tell WHR what specific data-security rules it purportedly violated. It is cold comfort to WHR (or other companies) that it will now have "an opportunity to represent to the finder of fact why it believes" its data-security practices met whatever data-security requirements the FTC announces during this litigation. Opp. 22. By announcing those requirements five years ***after*** WHR was attacked, the FTC denied WHR the opportunity to bring its data-security practices into line with the FTC's views of Section 5 ***before*** being subject to suit.

C. The FTC Has Not Alleged Substantial, Unavoidable Consumer Injury

The FTC rests its consumer-injury argument on its allegation that the attacks, which involved payment card information only, resulted in "$10.6 million in fraud loss." Am. Compl. ¶ 40. But the complaint stops short of alleging that this loss was borne by ***consumers*** or was not ***reasonably avoidable*** by consumers—necessary preconditions for FTC jurisdiction. That is because federal law and card-brand rules provide consumers with full reimbursement for unauthorized charges, MTD at

19-20, so the entire alleged loss either (i) was fully reimbursed to consumers; or (ii) could have been "reasonably avoid[ed]" by consumers by having their issuers rescind any unauthorized charges.

This is not, as the FTC argues, a "fact issue[]." Opp. 6. Even accepting as true the FTC's unsubstantiated allegation that some consumers might not have been reimbursed, *id*. at 8, federal law and card-brand zero-liability policies make clear that any such charges were nonetheless "reasonably avoidable" by consumers. Moreover, the FTC's claim that "federal law does not provide these same liability protections for debit cards" is flatly wrong. *Id.* As the FTC's own website makes clear, federal regulations eliminate all consumer liability for unauthorized charges on debit cards, so long as the charges are reported within 60 days. *See* 12 C.F.R. § 205.6(b)(3); http://www.consumer.ftc.gov//0213-lost-or-stolen-credit-atm-and-debit-cards.

With its unreimbursed-fraud argument blocked, the FTC ultimately resorts to arguing that its complaint alleges injuries "other than unreimbursed fraud," such as "frozen accounts" and "time and money resolving fraudulent charges." Opp. 5, 8. But courts in data-security cases have routinely rejected such incremental and attenuated injuries as actionable consumer harm—even in cases that do not apply the high "substantial injury" bar set by the FTC Act. *See Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 973 n. 18 (D.C. Cir. 1985); *Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1, 8 (D.D.C. 2007). Even the FTC has stated that the FTC Act, in most cases, requires concrete "monetary harm." *In re Int'l Harvester*, 1984 WL 565290, at *99 (FTC 1980).[5] Nor do *Reilly v. Ceridian*, 664 F.3d 38 (3d Cir. 2011) or *Anderson v. Hannaford Brothers Co.*, 659 F.3d 151 (1st Cir. 2011), support the FTC's arguments. The determinative factor in *Reilly* was that consumers' "credit card statements [were] exactly the same today as they would have been had [the defendant's] database never been hacked." 664 F.3d at 45. That is equally true here because federal law and

[5] *FTC v. Neovi, Inc.*, 604 F.3d 1150 (9th Cir. 2010), provides no support for the FTC. *Neovi* held, unremarkably, that the withdrawal of $400 million from consumers' accounts constituted "substantial" injury. The Court did not hold, and had no occasion to hold, that non-economic, nuisance-type injuries were also "substantial" consumer injuries under the FTC Act.

card-brand policies eliminate any consumer liability for unauthorized transactions. *Hannaford* arose solely under Maine law, 659 F.3d at 153-54, so the court had no opportunity to address whether such minor injury-avoidance costs constitute unavoidable "substantial injury" under the FTC Act.

D. The FTC's Unfairness Allegations Fail Federal Pleading Requirements

Although the FTC claims that it "alleges with specificity" several data-security failures in paragraph 24 of its Amended Complaint, these purportedly "specific[]" allegations of liability boil down to vague claims of unreasonableness. Opp. 4. The addition of technical jargon surrounding these claims of unreasonableness does not change that the complaint's allegations are nothing more than inadequate "legal conclusions couched as factual allegations." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). And despite expressing surprise at WHR's causation argument, WHR's alleged failure "to adequately inventory computers connected to [WHR's] network" is the ***only*** action the Commission identifies as a potential cause of consumer injury. Opp. 6. That allegation, however, is unsupported by any facts explaining how WHR's supposed inability to "physically locate" computers enabled hackers to exfiltrate payment card data.

II. THE COUNT I DECEPTION CLAIM MUST BE DISMISSED

The FTC's attempt to salvage its deception claim is no more convincing. The FTC insists that WHR's privacy policy was "deceptive" because it misrepresented the state of data security at the Wyndham-branded hotels. But the privacy policy does not make ***any*** representations about data security at the Wyndham-branded hotels—indeed, the policy ***expressly disclaims*** such representations. *See* D.I. 91-3 at 5. The FTC tries to overcome that disclaimer by arguing that "the data security failures … [at] the 'Wyndham-branded hotels' are actually data security failures on [WHR's] own network" because WHR "permitted computers with unreasonable data security measures on its network." Opp. 27-28. But the owner of one computer network does not assume responsibility for the data-security failures on another network merely by connecting to it—if that

were so, then any user that connected to the Internet would be on the hook for data-security failures of every other user on the internet. The FTC's "guilt by association" argument thus has no merit.

Nor can the FTC save its deception claim by arguing that WHR exercised "'actual control' over … [its] franchisees' data security practices." *Id.* at 28. The allegations in the complaint do not establish that WHR exercised the kind of "day-to-day" control that is necessary to assign vicarious liability to a franchisor. *Caprigilione v. Radisson Hotels Int'l.*, 2011 WL 4736310, at *3 (D.N.J. 2011). And even assuming that they did, the privacy policy disclaims responsibility for data-security practices at the hotels without regard to whether WHR actually controls those practices or not.

The FTC insists that the Court must ignore the express disclaimer in WHR's privacy policy because the "effectiveness of such a disclaimer is a fact-specific inquiry" that is "inappropriate for a motion to dismiss." Opp. 30. But this is not a case in which a disclaimer is buried in fine print or otherwise obscured. The disclaimer in WHR's privacy policy is set forth in its own paragraph, with its own bold-face heading, using the same size and type of font used elsewhere in the document. Courts have relied on similar disclaimers to dismiss deception or fraud-based claims. *See, e.g.*, *Pathfinder Mgmt., Inc. v. Mayne Pharma PTY*, 2008 WL 3192563, at *16 (D.N.J. 2008); *Eckler v. Wal-Mart Stores, Inc.*, 2012 WL 5382218, at *7 (S.D. Cal. 2012).

The FTC cannot manufacture ambiguity in the express disclaimer by selectively quoting two snippets from the privacy policy out of context. *See* Opp. 29. The first quote relied on by the FTC merely restricts the geographic scope of the policy to "residents of the United States, hotels of our brands in the United States, and Loyalty Program activities in the United States." That language no more suggests that WHR is assuming responsibility for the data-security practices of "hotels" than it does that WHR is assuming responsibility for the data-security practices of "residents." The second quote merely states that WHR "recognizes the importance of … information collected about guests."

The policy clearly explains, however, that it applies only to information that ***WHR*** "collect[s] about guests," not to information that "[e]ach Franchisee collects" from guests.

The FTC devotes only one sentence to defending the complaint's conclusory allegations about WHR's own data-security practices. *See* Opp. 28. Those bare legal assertions fall short of federal pleading requirements and should be disregarded on a motion to dismiss. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Although its deception claim hinges on proving that WHR's data-security practices were not "industry standard" or "commercially reasonable," the FTC does not dispute that its complaint contains ***no allegations at all*** explaining what data-security practices were "standard" in the hospitality industry in 2008 or how WHR fell short of that benchmark.

Dated: June 10, 2013

Respectfully submitted,

By: s/ Jennifer A. Hradil

Jennifer A. Hradil, Esq.
Justin T. Quinn, Esq.
GIBBONS P.C.
One Gateway Center
Newark, NJ 07102-5310
(973) 596-4500

Eugene F. Assaf, P.C., DC Bar 449778
Pro Hac Vice
K. Winn Allen, DC Bar 1000590
Pro Hac Vice
KIRKLAND & ELLIS, LLP
655 Fifteenth St. N.W.
Washington, D.C. 20005
(202) 879-5078
eugene.assaf@kirkland.com
winn.allen@kirkland.com

Douglas H. Meal, MA Bar 340971
Pro Hac Vice
ROPES & GRAY, LLP
Prudential Tower, 800 Boylston Street
Boston, MA 02199-3600
(617) 951-7517
douglas.meal@ropesgray.com

Attorneys for Defendants